REMARKS

This amendment is responsive to the Office Action dated May 14, 2007. Applicant has amended claim 6 and added claim 56.

Claim Rejection Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 1–3, 6–11, 15, 22–24, 26–31, and 35 under 35 U.S.C. § 103(a) as being unpatentable over Valois et al. (US 2004/0260818, "Valois") in view of Delany et al. (US 2002/0156879, "Delany"). The Examiner rejected claim 4 under 35 U.S.C. § 103(a) as being unpatentable over Valois as applied to claims 1–3, 15, 22–24, and 35, and further in view of Mitra (US 6,973,460). The Examiner also rejected claims 12–14, 19–21, and 32–34 under 35 U.S.C. § 103(a) as being unpatentable over Valois in view of Delany, and further in view of Nelson et al. (US 6,243,713, "Nelson"). Applicant respectfully traverses the rejection. The applied references fail to teach, suggest, or disclose the inventions defined by Applicant's claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention.

Applicant's claims recite techniques for controlling access to resources within a device by a client. The claims require two levels of access control. Moreover, Applicant's claims require that the authorization data for resources in the network device define both of these levels. First, the claims require that authorization data for a resource define a "course-grain access control attribute defining access control rights for the resource." Separately, the claims also require that same authorization data further define a regular expression that is used to evaluate a text-based command *provided by the client* to access that particular resource. The claims require controlling access to configuration data for the resource based on both of these recited features, i.e.., controlling access to the configuration data for the resource based on the coarse-grain access control attribute that defines access control rights for the *resource* as well as the evaluation of the command from the client requesting access to the configuration data.

These elements are specifically set forth in claim 1. For example, Applicant's claim 1 requires storing authorization data that defines an access control attribute and an associated regular expression specifying a textual pattern, wherein the access control attribute is a coarse-grain access control attribute defining access control rights for a resource provided by a device.

Claim 1 also requires receiving a command from a client, wherein the command requests access to configuration data for the resource of the device. Moreover, claim 1 requires evaluating the command using the regular expression to determine whether the command matches the textual pattern, and controlling access to the configuration data by the client based on the coarse-grain access control attribute and the evaluation of the regular expression. That is, claim 1 specifically requires that access to configuration data by a client is based on use of regular expressions to evaluate of a command to access the configuration data as issued by that client as well as the access control attribute associated with the resource.

In the Office Action, the Examiner cited Valois in view of Delany in support of the rejection of claim 1. The Examiner stated that it would be obvious to modify the Valois system based on the teachings of Delany to achieve Applicant's claimed invention.

In general, Valois describes a verification software system that uses test scripts to test the security policies of a network device, and to verify that the device implements its intended security policy. Valois, Abstract. Delany generally discloses a policy, associated with a group, that controls user subscription to and unsubscription from the group. Delany, Abstract.

To be clear, Valois discloses using "test scripts" as part of a verification software system to determine whether a configuration file of a network device "passes" or "fails" each script. Valois, ¶ [0024]. The test scripts include a security characteristic or policy for testing the different network devices. Valois, ¶ [0055]. Valois further states that the execution of each test script is performed offline, i.e., while the network device **is not active**. Valois, ¶ [0025]. Valois describes that these test scripts of the verification software system may utilize regular expressions to search configuration files of the network devices to verify compliance with the desired security policies. Valois, ¶ [0057]–[0058].

Delany describes using policy domains and policies to make authentication and authorization decisions. Delany, ¶ [0118]. These decisions are made regarding requests to access a resource provided by a network. Delany, ¶ [0115]. A resource, as described by Delany, is "anything that is possible to address with a uniform resource locator." Delany, ¶ [0098]. Delany states that a host name is "the name of the machine on which the resource resides," Delany, ¶ [0099] and a URL prefix is a "complete path, or a cropped portion thereof" following the host name, Delany, ¶ [0102]. Delany further states that a policy domain is "a logical grouping of Web Server host ID's, host names, URL prefixes, and rules." Delany, ¶ [0118]. Moreover, Delany states that host names and URL prefixes are the "course-grain [sic] portion of the web name space a given policy domain protects." *Id.*

In the Office Action, the Examiner cited the test scripts of Valois as disclosing storing authorization data that defines an access control attribute and an associated regular expression specifying a textual pattern. The Examiner admitted, that Valois fails to teach or suggest that the access control attribute is a coarse-grain access control attribute defining access control rights for a resource provided by a device, but argued that the host name and URL prefixes of Delany disclose this requirement of Applicant's claim 1. Thus the Examiner's argument is that it would have been obvious for one of ordinary skill in the art to modify the <u>offline-executed test scripts of Valois</u>, which are used to test whether a single device is configured properly, to use the URL prefixes of Delany that describe the portion of a network that a given policy domain protects. Even if one skilled in the art had been motivated to so combine the references as suggested by the Examiner, one would not have arrived at a system that remotely satisfies the requirements of Applicant's claim 1.

For example, Valois in view of Delany fails to teach, suggest, or disclose storing authorization data that defines both an access control attribute and an associated regular expression specifying a textual pattern, wherein the access control attribute is a coarse-grain access control attribute defining access control rights for a resource provided by a device. Contrary to the Examiner's assertion, Valois fails to teach or suggest storing authorization data that defines an access control attribute and an associated regular expression specifying a textual pattern. The regular expression of Valois, i.e. a GREP command, is merely used to search files. Valois never teaches that such GREP commands are used as access control attributes to control access to specific resources. Instead, Valois teaches test scripts that may use a regular expression *to search configuration files*. A test script that searches configuration files is not an access control attribute because a test script does not define access control rights for a resource provided by a device. A test script is merely a way of testing the configuration of a device to determine whether the access control lists (ACLs) on the device satisfy corporate policies.

The Examiner fails to understand that the test scripts of Valios are not defined by any authorization data for a resource of a network device. Valois [0058] clearly describes a configuration file on the network device that references one or more of access control lists to control access to the resources of the device. In this well-known approach, the configuration file and the ACLs referenced by the configuration file constitute the authorization data in Valois. Applicant's claims require that the authorization data **define the coarse-grain access control attribute** as well as the register expression itself that is used to control access to a resource. In Valois, neither the configuration file nor the ACLs in any way define or make reference to the test scripts. Nor do the test scripts execute so as to control access to the resource specified by the configuration file upon receiving from a client a command to access the resource, as required by claim 1. Quite the contrary, Valois [0058] makes very clear that the test scripts are merely offline-scripts that parse a configuration file to identify references to access control lists and verify that the ACLs conform with corporate policies.

In the Examiner's footnote 1, pg. 3, the Examiner states "Authorization data corresponds to "references" and the definition is an attribute that is part of the Access Control List (ACL)." Applicant finds this sentence unclear. To the best Applicant can understand, this further emphasizes the Examiner's misunderstanding. In Valois, it is the configuration file that "references" the access control lists for the network device, and the access control lists define access control attributes. None of this defines a regular expression specifying a textual pattern for evaluating a command received from a client, as required by claim 1. The Valois test scripts are scripts that execute off-line to check the configuration file and the access control lists. The authorization data of the Valois device is entirely unaware of, and does not define, the test scripts. Morever, in no way are the test scripts of Valois used to evaluate a command from a client nor is there any suggestion of this feature. Quite clearly the test scripts in Valois process the configuration file and the access control lists referenced by the configuration file to determine whether the ACLs comply with policies. This is entirely different from authorization data that defines a regular expression specifying a textual pattern for evaluating a command received from a client, as required by claim 1. The Valois test scripts are not defined by authorization data of a device; nor are the test scripts even capable of evaluating a command received by a client.

Furthermore, contrary to the Examiner's assertions, Delany fails to disclose or suggest authorization data that defines an access control attribute that defines access control rights for a resource provided by a device. Specifically, Delany describes use of host names and URL prefixes to specify "a coarse-grain portion of the web name space" that a given policy domain protects. Application of this teaching as suggested by the Examiner is seriously flawed

First, modification of Valois as suggested by the Examiner would simply result in the network devices utilizing host names and URL prefixes. A web name space or a portion thereof is not an access control attribute as claimed by the Applicant. Applicant's claim 1 requires that the coarse-grain access control attribute is *defined by authorization data* of a network device. Moreover, claim 1 requires that the authorization data be associated with a specific resource of the network device. An access control attribute, as expressly required by Applicant's claim 1, is defined by authorization data of a device and defines access control rights for a resource provided by that device. Delany states that a policy domain is used to protect the web name space, and that the URL prefix and host name define the coarse-grain portion of the web name space, not the policy domain. Delany fails to teach or suggest authorization data of a network device that defines a coarse-grain access control attribute defined by authorization data of a device. Moreover, Delany fails to teach or suggest a coarse-grain access control attribute defining access control rights for a resource provided by a device. Therefore, as both Valois and Delany individually fail to teach or suggest these requirements, Valois in view of Delany certainly fails to teach these requirements.

Furthermore, Valois in view of Delany also fails to teach or suggest receiving a command from a client, wherein the command requests access to configuration data for the resource of the device as required by Applicant's claim 1. The Examiner cited Delany at ¶¶ [0159], [0165] as disclosing this requirement. These paragraphs of Delany describe receiving a request to access Configure tab 416 and performing attribute access control, e.g., controlling who has view and modify permissions for each attribute. Delany states that, with respect to an attribute, "[a]n identity profile is a set of information associated with a particular entity. The data elements of the identity profile are called attributes." Delany, ¶ [0107]. **Applicant respectfully points out that claim 1 specifically requires that the resource of the device for which the command requests access is the same resource of the same device for which the access control**

attribute defines access control rights. The "access control attribute" cited by the Examiner with respect to the first element of Applicant's claim 1 was the "course-grain [sic] portion of a web name space," i.e. the resources locatable via a URL. The Examiner cannot now argue that the access control attribute is instead an identify profile having a set of data elements associated with a particular entry. The two elements cited by the Examiner are entirely different. The Examiner has pointed to no feature taught by Delany or Valois that satisfies the requirements of Applicant's claim. The Examiner characterizes to URL prefixes and hostnames as a coarse-grain attribute with respect to certain elements of claim 1, then tries to argue that an identify profile is a coarse-grain attribute.

Moreover, Delany discloses receiving a command from a client with one device to access <u>a different resource of a different device</u>. The first device, which receives the command, controls access for various resources located across the network <u>on different devices</u>, as discussed in Delany. Valois fails to disclose receiving any sort of command from a client in any form. Therefore, Valois in view of Delany fails to teach, suggest, or disclose receiving a command from a client, wherein the command requests access to configuration data for the resource of the device.

Valois in view of Delany likewise fails to teach, suggest, or disclose evaluating the command using the regular expression to determine whether the command matches the textual pattern. As Valois in view of Delany fails to teach, suggest, or disclose receiving a command, the references necessarily fail to disclose evaluating the command. However, even if the references had taught receiving the command, they would still fail to teach evaluating the command using a regular expression that is defined within authorization data of the device. Valois teaches regular expressions used to search a configuration file. There is no teaching, suggestion, or disclosure in either Valois or Delany as to how one could use a regular expression designed for searching a file (e.g., GREP), and modify it to evaluate to evaluate a command from a client. GREP is designed to search a file based on a textual pattern and print the lines that match the pattern. It is entirely unclear how one of ordinary skill in the art could modify GREP to evaluate a command from a client according to the teachings of Valois and Delany. Thus Valois in view of Delany fails to teach, suggest, or disclose evaluating the command using the regular expression to determine whether the command matches the textual pattern.

Likewise, as Valois in view of Delany fails to teach, suggest, or disclose the elements of Applicant's claim 1 as discussed above, Valois in view of Delany necessarily fails to teach, suggest, or disclose controlling access to the configuration data by the client based on the coarse-grain access control attribute and the evaluation of the regular expression.

Claim 21 comprises requirements similar to those of claim 1, therefore similar arguments apply to the requirements of claim 21. Claim 19 requires receiving input defining an access control attribute and an associated regular expression that specifies a textual pattern and evaluating a command using the regular expression. These requirements are similar to their counterparts of claim 1, therefore similar arguments apply. However, in addition, claim 19 requires pre-processing the regular expression to automatically insert one or more meta-characters into the regular expression and that a client enters the command via a command line interface.

The Examiner admitted that Valois in view of Delany fails to disclose pre-processing the regular expression to automatically insert one or more meta-characters into the regular expression. However, the Examiner cited Nelson at col. 10, ll. 39–50 as disclosing this requirement, arguing that it would have been obvious for one of ordinary skill in the art to combine Valois, Delany, and Nelson to arrive at this requirement of Applicant's claim 19.

The Examiner cited Nelson, col. 9, ll. 60–65,[1] which state, "Generally, the purpose of pre-processing is to convert a single block of component data into a list 660 of tokens that represent the original data of the component, each with additional reference data, which tokens will be stored in the multimedia index 140. Thus, pre-processing may be understood **to perform a data reduction or abstraction function**." Applicant's claim 19 does not require data reduction or abstraction. To quite the contrary, claim 19 requires <u>insertion</u> of one or more meta-characters as a result of the pre-processing. One skilled in the art would readily appreciate that insertion of data is not data reduction or abstraction.

The cited portion of Nelson describes pre-processing text input to tokenize the text input. The purpose of the tokenization is to abstract the data. A tokenized regular expression is not at all useful for evaluating a command in real-time using the regular expression. If the regular

[1] The Examiner cited this portion of Nelson in support of the rejection of claim 12, which recites a requirement similar to this requirement of claim 19. Office Action dated 05-14-2007, p. 8.

expression were tokenized, it would be impossible to evaluate the command in real-time using the regular expression because the tokenized regular expression would first need to be de-tokenized (i.e. reassembled) before it could be executed. Nelson does not describe such a de-tokenization procedure, mostly because Nelson is directed to using the tokenized input to perform an indexing function. *See, e.g.*, Nelson, Abstract.

Claim 19 also requires pre-processing the regular expression to automatically insert one or more meta-characters into the regular expression. The Examiner cited Delany, ¶¶ [0451]–[0453] as disclosing inserting one or more meta-characters into the regular expression. However, these cited paragraphs do not disclose inserting anything into a regular expression, or any form of input. Instead, they describe pre-existing meta-characters used by a policy. None of the references, i.e. Valois, Delany, or Nelson, describe automatically inserting **anything** into the input, especially when the input is a regular expression. Therefore, Valois, in view of Delany, and in further view of Nelson fails to teach, suggest, or disclose pre-processing the regular expression to automatically insert one or more meta-characters into the regular expression. Claims 12, 20, and 32 comprise similar requirements to pre-process the regular expression to automatically insert one or more meta-characters into the regular expression, therefore similar arguments apply to claims 12, 20, and 32.

The references also fail to teach, suggest, or disclose evaluating a command in real-time using the regular expression as a client enters the command via a command line interface. The Examiner cited the graphical user interface (GUI) of Delany as disclosing a command line interface.[2] A GUI is dynamically opposed to a command line interface. It is entirely unclear how a command line interface "corresponds to [a] 'GUI.'" With a command line interface, a user can only enter text. With a GUI, a user views and interacts with graphic objects. Valois, Nelson, and Delany each fail to disclose evaluating a command as a client enters the command via a command line interface, therefore Valois in view of Delany and in further view of Nelson fails to teach, suggest, or disclose this requirement of claim 19. Claims 7 and 27 comprise similar requirements respectively of a command line interface, thus similar arguments apply to claims 7 and 27.

[2] The Examiner stated in an Examiner's note, with respect to the rejection of claim 7, that the command line interface "corresponds to 'GUI'". Office Action dated 05-14-2007, pp. 5–7 n. 2; *see also* Office Action, pp. 9–10.

The claims dependent on independent claims 1, 19, and 22, namely claims 2–4, 6–15, 20–21, 23–24, and 26–35, incorporate all of the limitations of the respective base claims, and therefore are patentable for at least the reasons expressed above. Moreover, the dependent claims recite a number of additional features that are likewise not taught or suggested by Valois in view of Delany or in further view of Nelson.

As one example, claim 2 requires allowing access to the configuration data when the access control attribute denies access to the resource and the textual pattern of the regular expression matches the command. The Examiner argues that hostnames and URL prefixes are coarse-grain access control attributes. *How could the Valois system be modified to allow access when the coarse-grain access control attribute* ***denies access*** *but the textual pattern of the regular expression matches the command, as specified in claim 2.* If a URL does not provide access a device, how could this be overridden, as required by claim 2?

As another example, claim 6 requires wherein the coarse-grain access control attribute comprises a set of permission bits, and each of the permission bits is associated with a respective group of the resources *within the network device*. In the Office Action, the Examiner cited ¶ [0161] of Delany as disclosing this requirement of claim 6. **However, this cited portion of Delany says nothing of a permission bit being associated with a respective group of resources.** The cited portion merely describes the general notion of access control as disclosed by Delany. The word "bits" does not even occur in the specification of Delany. Likewise, the word "bits" does not occur in the specification of Valois. Therefore Valois in view of Delany fails to teach or suggest wherein the coarse-grain access control attribute comprises a set of permission bits, and each of the permission bits is associated with a respective group of the resources. Moreover, the Examiner previously argued that the URL prefixes and hosts names are coarse-grain access control attributes defined by authorization data. The The URL prefixes and host names of Delany could not comprise **permission bits associated with groups of resource** ***within the network device***. Claim 26 comprises a similar requirement for which similar arguments apply.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims 1–4, 6–15, 19–24, and 26–35 under 35 U.S.C. § 103(a).

Applicant respectfully requests withdrawal of these rejections and allowance of all pending claims.

New Claims:

Applicant has added claim 56 to the pending application. The applied references fail to disclose or suggest the inventions defined by Applicant's new claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed inventions. As one example, the references fail to disclose or suggest that a resource is at least one of a present configuration of the device, policies and relationships with other devices, a configuration of an interface card of the device, a parameter for network protocols supported by the device, a specification for a physical component within the device, information maintained by the device, a software module executing on the device, device chassis inventory, device system parameters, routing policies, forwarding options, network flow statistics, error logs, user information, or performance metrics, as required by claim 56. No new matter has been added by the new claims. Support for this new claim can be found, e.g., in Applicant's specification, ¶ [0003].

CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date: 11/20/2007

SHUMAKER & SIEFFERT, P.A.
1625 Radio Drive, Suite 300
Woodbury, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

By:

Name: Kent J. Sieffert
Reg. No.: 41,312